Q4 Company

NEWS RELEASE

Opus Security Elevates Vulnerability Management With its AI-Powered Multi-Layered Prioritization Engine

2024-09-11

PALO ALTO, Calif., Sept. 11, 2024 (GLOBE NEWSWIRE) -- Opus' innovative engine integrates AI-driven intelligence, contextual data and automated decision-making to drive precise, efficient vulnerability remediation.

Opus Security, the leader in unified cloud-native remediation, today announced the launch of its Advanced Multi-Layered Prioritization Engine, designed to revolutionize how organizations manage, prioritize and remediate security vulnerabilities. Leveraging AI-driven intelligence, deep contextual data and automated decision-making capabilities, this innovative engine helps organizations prioritize the most critical vulnerabilities, enhancing both security posture and operational efficiency.

A Breakthrough in Vulnerability Remediation

Security teams are overwhelmed by the need to rapidly prioritize alerts from multiple tools across various attack surfaces. These may include redundant alerts or negligible findings and teams must decide which to address first without adequate information, context and ability to do so. Security teams struggle to identify and address the most critical issues, and developers have limited time and scope to devote to security fixes—especially when it isn't clear what is important and what is negligible. Developers are often bombarded with alerts that are duplicates or irrelevant due to inefficient prioritization—wasting time and increasing friction and frustration.

Opus Security's Advanced Multi-Layered Prioritization Engine is a transformative approach to vulnerability management. By integrating multiple layers of intelligence, contextual analysis and risk mitigation, the engine ensures that security teams can effectively prioritize and address the most critical vulnerabilities, reducing risk, enhancing operational efficiency and supporting overall business goals. The engine integrates traditional vulnerability severity scoring with dynamic exploitability analysis, detailed environmental context and an automated decision-making process to provide a robust method for ranking vulnerabilities.

A key component of this engine is the AI-Based Vulnerability Intelligence Layer, which goes beyond traditional severity scoring. This layer leverages over 700 real-time threat intelligence feeds to build a deep and nuanced understanding of each vulnerability's risk. By incorporating intelligence from sources such as dark web forums, social media, open-source tools, exploit databases and active threat campaigns, the engine can flag high-risk issues with unparalleled accuracy. This intelligence-driven approach ensures that organizations are aware of vulnerabilities and their likelihood of exploitation in the wild, allowing for proactive and informed remediation efforts.

Using a five-layered framework, the engine first performs a Base Severity Assessment, aggregating severity scores from leading security tools and public databases to ensure that no critical vulnerabilities are overlooked. Next, the AI-Based Vulnerability Intelligence layer leverages real-time threat intelligence to flag high-risk issues based on their likelihood of exploitation. The Contextual Impact layer then prioritizes vulnerabilities according to their relevance to specific business functions, protecting critical systems first, especially those that handle sensitive data. The engine is the first to enable real SSVC decision-making, fully baked into the product. This helps teams categorize vulnerabilities into specific response actions based on the affected environment's severity, exploitability and criticality. Finally, the Risk Customization layer allows organizations to tailor prioritization according to their unique risk appetite and operational needs.

Additionally, Opus Security introduces Effortless Data Querying, allowing users to interact with the platform using natural language. This feature enables users to quickly refine vulnerability lists based on specific concerns and make precise, data-driven decisions by leveraging advanced AI-powered insights.

Driving Value and Operational Excellence

The engine's multi-layered approach ensures unprecedented precision in risk management by integrating real-time intelligence with detailed contextual analysis. This integration enables SSVC decision-making, allowing security teams to focus on vulnerabilities that truly matter, reducing the likelihood of overlooking critical vulnerabilities.

Opus aligns security decisions with business priorities by deeply understanding the organization's structure, critical services and risk profiles, driving context-aware decision-making that protects critical assets and directly supports strategic goals.

"Opus' new Advanced Multi-Layered Prioritization Engine is a game-changer in vulnerability remediation, simplifying, streamlining and optimizing the process considerably. The engine's ability to prioritize the vulnerabilities that pose the greatest risk reduces overall security costs and helps security and developer teams avoid unnecessary remediation of low-risk issues," said Meny Har, CEO of Opus Security. "Minimizing friction between development and security teams, driving smoother collaboration and ensuring that security measures do not impede the development process means that all teams can focus on what matters and fix what counts."

About Opus Security

Opus Security is at the forefront of cloud-native vulnerability remediation, delivering solutions that streamline remediation across complex IT ecosystems. Opus Security provides unparalleled visibility and control over vulnerabilities by integrating existing security tools and enhancing them with advanced AI and contextual intelligence. The platform's innovative features, including the new Advanced Multi-Layered Prioritization Engine, empower organizations to protect their most critical assets with confidence and precision.

For more information about Opus Security and its solutions, visit **https://www.opus.security/**.

Contact

Senior Account Executive
Hannah Sather
Montner Tech PR
hsather@montner.com

Source: Opus Security